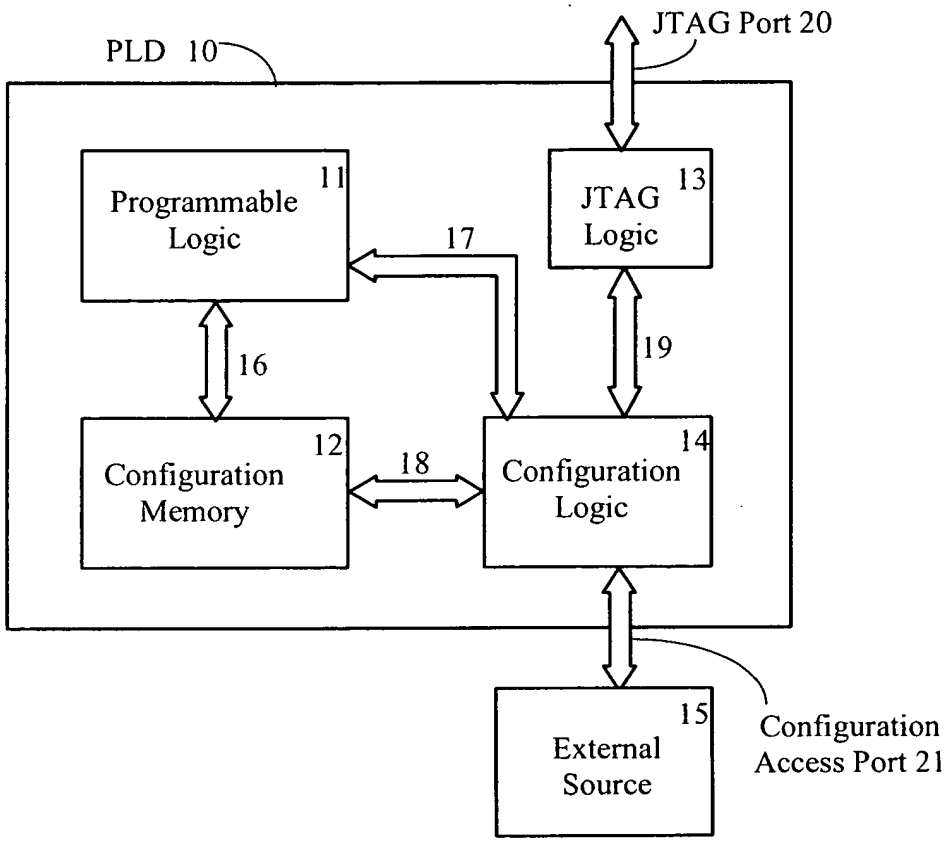


Fig. 1
PRIOR ART

Header A
Data A
Header B
Data 1B
Data 2B
Data 3B
Data 4B
Header C
Data 1C
⋮

Fig. 2a
PRIOR ART

Bitstream header Config. Logic Reg. address	Config. Logic Register data contents
0000	Cyclic Redundancy Check (CRC)
0001	Frame Address
0010	Frame Data Input
0011	Frame Data Output
0100	Command
0110	Control
0111	Status
1000	Daisy Chain Output
1001	Configuration Option
1010	Reserved
1011	Frame Length
1100	Reserved
1101	Reserved
1110	Reserved
1111	Reserved

Fig. 2d
PRIOR ART

32-bit Command Header Format 1

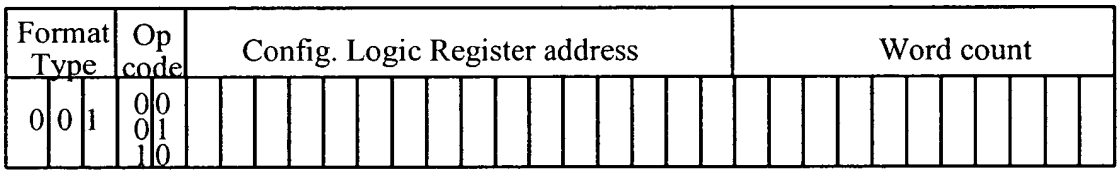
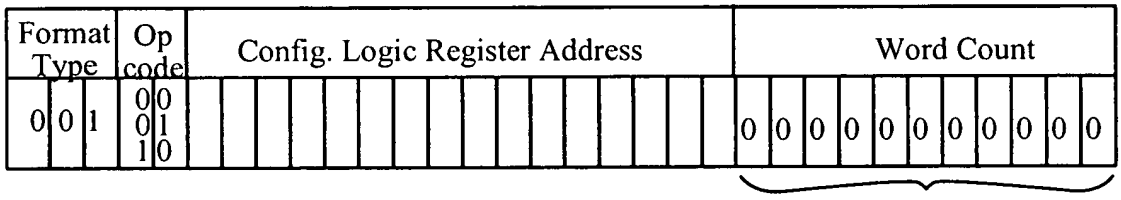


Fig. 2b PRIOR ART

32-bit Command Header Format 1



32-bit Command Header Format 2

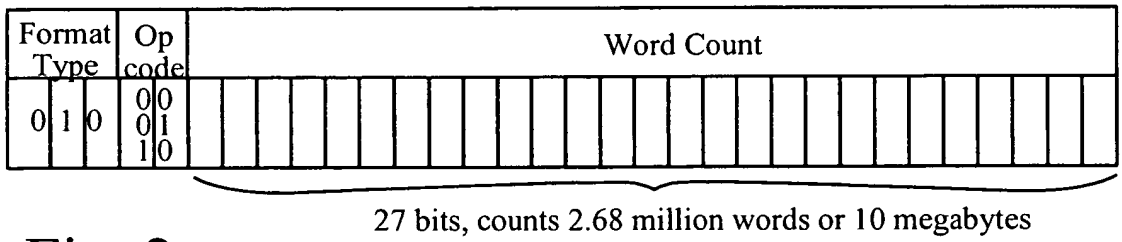


Fig. 2c PRIOR ART

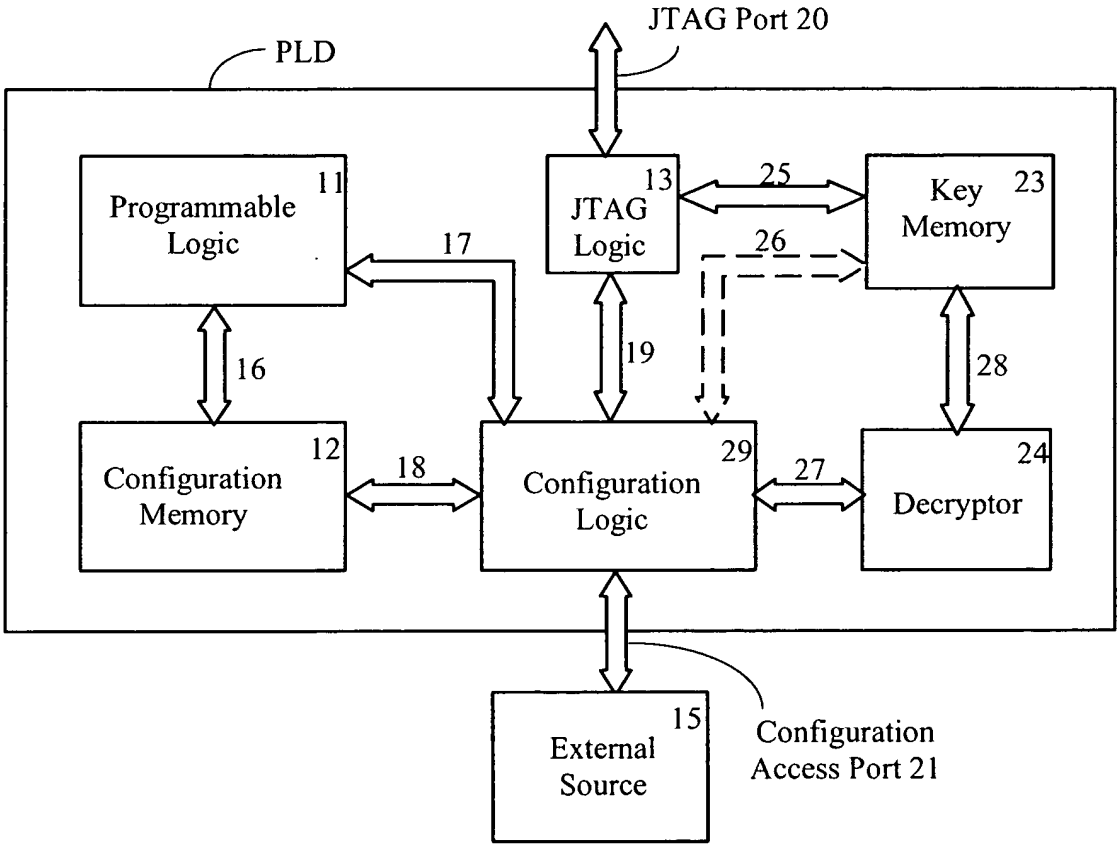

JTAG Port 20
PLD
Programmable Logic
11
JTAG Logic
13
25
Key Memory
23
17
26
16
19
28
Configuration Memory
12
18
Configuration Logic
29
27
Decryptor
24
External Source
15
Configuration Access Port 21

Fig. 3

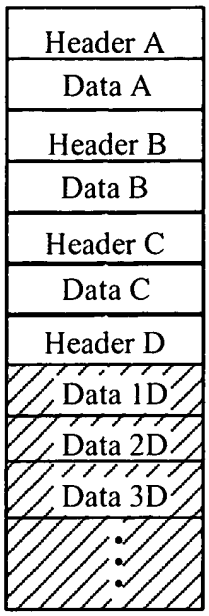


Fig. 4a

Bitstream header Config. Logic Reg. address	Config. Logic Register data contents
0000	Cyclic Redundancy Check (CRC)
0001	Frame Address
0010	Frame Data Input
0011	Frame Data Output
0100	Command
0110	Control
0111	Status
1000	Daisy Chain Output
1001	Configuration Option
1010	Reserved
1011	Frame Length
1100	Cipher block chaining(CBC) starter
1101	Initial key address
1110	Reserved
1111	Reserved

Fig. 4d

32-bit Command Header Format 1

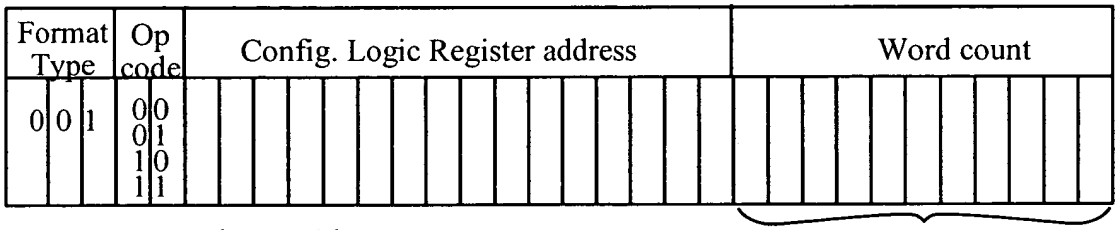
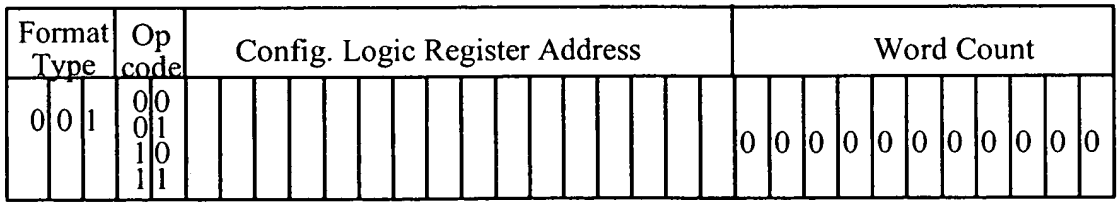


Fig. 4b

32-bit Command Header Format 1



32-bit Command Header Format 2

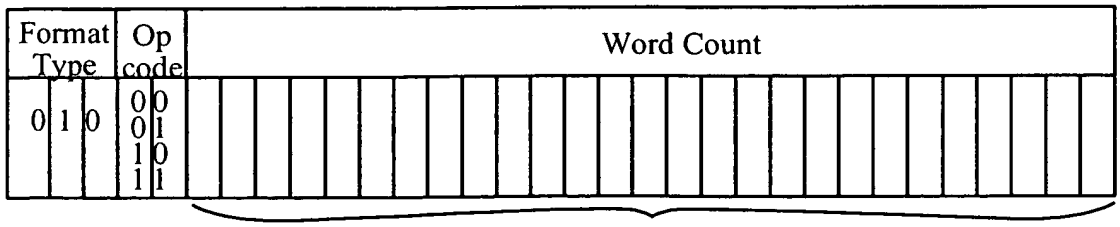


Fig. 4c

UNENCRYPTED VERSION

```
                    Dummy word 11111111111111111111111111111111
                     Sync word 10101010100110010101010101100110
Type 1 write 1 words to CMD  001100000000000010000000000000001
                  RCRC command 00000000000000000000000000000111
Type 1 write 1 words to FLR  001100000000000101100000000000001
                  data word 0 00000000000000000000000000011001
Type 1 write 1 words to COR  001100000000000100100000000000001
                  data word 0 00000000000010000011111111000001
Type 1 write 1 words to ID   001100000000000111000000000000001
                  data word 0 00000010000000010000000010010011
Type 1 write 1 words to MASK 001100000000000011000000000000001
                  data word 0 00000000000000000000000000000000
Type 1 write 1 words to CMD  001100000000000010000000000000001
                SWITCH command 00000000000000000000000000001001
Type 1 write 1 words to FAR  001100000000000000100000000000001
                  data word 0 00000000000000000000000000000000
Type 1 write 1 words to CMD  001100000000000010000000000000001
                  WCFG command 00000000000000000000000000000001
Type 1 write 0 words to FDRI 001100000000000001000000000000000
Type 2 write 10530 words to FDRI 010100000000000000101001001000010
                  data word 0 00000000000000000000000000000000
                  data word 1 00000000000000000000000000000000
                  data word 2 00001000000000000000000000000000
                  data word 3 00001000000000011111111111111100
                                          .
                                          .
                                          .
                 data word 10526 00000000000000000000000000000000
                 data word 10527 00000000010000000000000000000001
                 data word 10528 00000000000000000000000000000000
                 data word 10529 00000000000000000000000000000000
                   Auto CRC word 00000000000000000110111000010001
Type 1 write 1 words to CMD  001100000000000010000000000000001
                  LFRM command 00000000000000000000000000000011
                  Type 1 NO OP 00100000000000000000000000000000
                                          .
                                          .
                                          .
                  Type 1 NO OP 00100000000000000000000000000000
Type 1 write 1 words to COR  001100000000000100100000000000001
                  data word 0 00000001000001000000111111000001
Type 1 write 1 words to CMD  001100000000000010000000000000001
                 START command 00000000000000000000000000000101
Type 1 write 1 words to CTL  001100000000000010100000000000001
                  data word 0 00000000000000000000000000000000
Type 1 write 1 words to CMD  001100000000000010000000000000001
               GRESTORE command 00000000000000000000000000001010
Type 1 write 1 words to CRC  001100000000000000000000000000001
                  data word 0 00000000000000000010100100110010
Type 1 write 1 words to CMD  001100000000000010000000000000001
               DESYNCH command 00000000000000000000000000001101
                  Type 1 NO OP 00100000000000000000000000000000
```

Fig. 5a

ENCRYPTED VERSION

```
                    Dummy word 11111111111111111111111111111111
                     Sync word 10101010100110010101010101100110
  Type 1 write 1 words to CMD  00110000000000001000000000000001
                   RCRC command 00000000000000000000000000000111
  Type 1 write 1 words to FLR  00110000000000010110000000000001
                     data word 0 00000000000000000000000000011001
  Type 1 write 1 words to COR  00110000000000010010000000000001
                     data word 0 00000000000001000011111111000001
  Type 1 write 1 words to ID   00110000000000011100000000000001
                     data word 0 00000010000000010000000010010011
  Type 1 write 1 words to MASK 00110000000000011000000000000001
                     data word 0 00000000000000000000000000000000
  Type 1 write 1 words to CMD  00110000000000010000000000000001
                  SWITCH command 00000000000000000000000000001001
  Type 1 write 1 words to FAR  00110000000000000010000000000001
                     data word 0 00000000000000000000000000000000
  Type 1 write 1 words to CMD  00110000000000010000000000000001
                    WCFG command 00000000000000000000000000000001
Type 1 write 1 word to KEY ADDR 00110000000000011000000000000001
                     data word 0 00000000000000000000000000000000
  Type 1 write 2 words to CBC  00110000000000011010000000000010
                     data word 0 10010000101010111100110111101111
                     data word 1 00010010001101000101011001111000
 Type 1 decrypt 0 words to FDRI 00111000000000000100000000000000
 Type 2 dec 10530 words to FDRI 01011000000000000010100100100010
                     data word 0 00010101110110110011001011001000
                     data word 1 11100000111000110111111101100111
                     data word 2 10101010011111011110001100110011
                     data word 3 01100001101011100001011010110100
                                 .
                                 .
                                 .
                data word 10526 01011001101111101100010101001010
                data word 10527 00101001010111111101011110110000
                data word 10528 11000000001010100110011000101010
                data word 10529 01111111110010000001100011100010
                  Auto CRC word 00000000000000001011111011001010
  Type 1 write 1 words to CMD  00110000000000010000000000000001
                   LFRM command 00000000000000000000000000000011
                   Type 1 NO OP 00100000000000000000000000000000
                                 .
                                 .
                                 .
                   Type 1 NO OP 00100000000000000000000000000000
  Type 1 write 1 words to COR  00110000000000010010000000000001
                     data word 0 00000000000001000011111111000001
  Type 1 write 1 words to CMD  00110000000000010000000000000001
                   START command 00000000000000000000000000000101
  Type 1 write 1 words to CTL  00110000000000010100000000000001
                     data word 0 00000000000000000000000000000000
  Type 1 write 1 words to CMD  00110000000000010000000000000001
                GRESTORE command 00000000000000000000000000001010
  Type 1 write 1 words to CRC  00110000000000000000000000000001
                     data word 0 00000000000000000001010111001111
  Type 1 write 1 words to CMD  00110000000000010000000000000001
                DESYNCH command 00000000000000000000000000001101
                   Type 1 NO OP 00100000000000000000000000000000
```

Fig. 5b

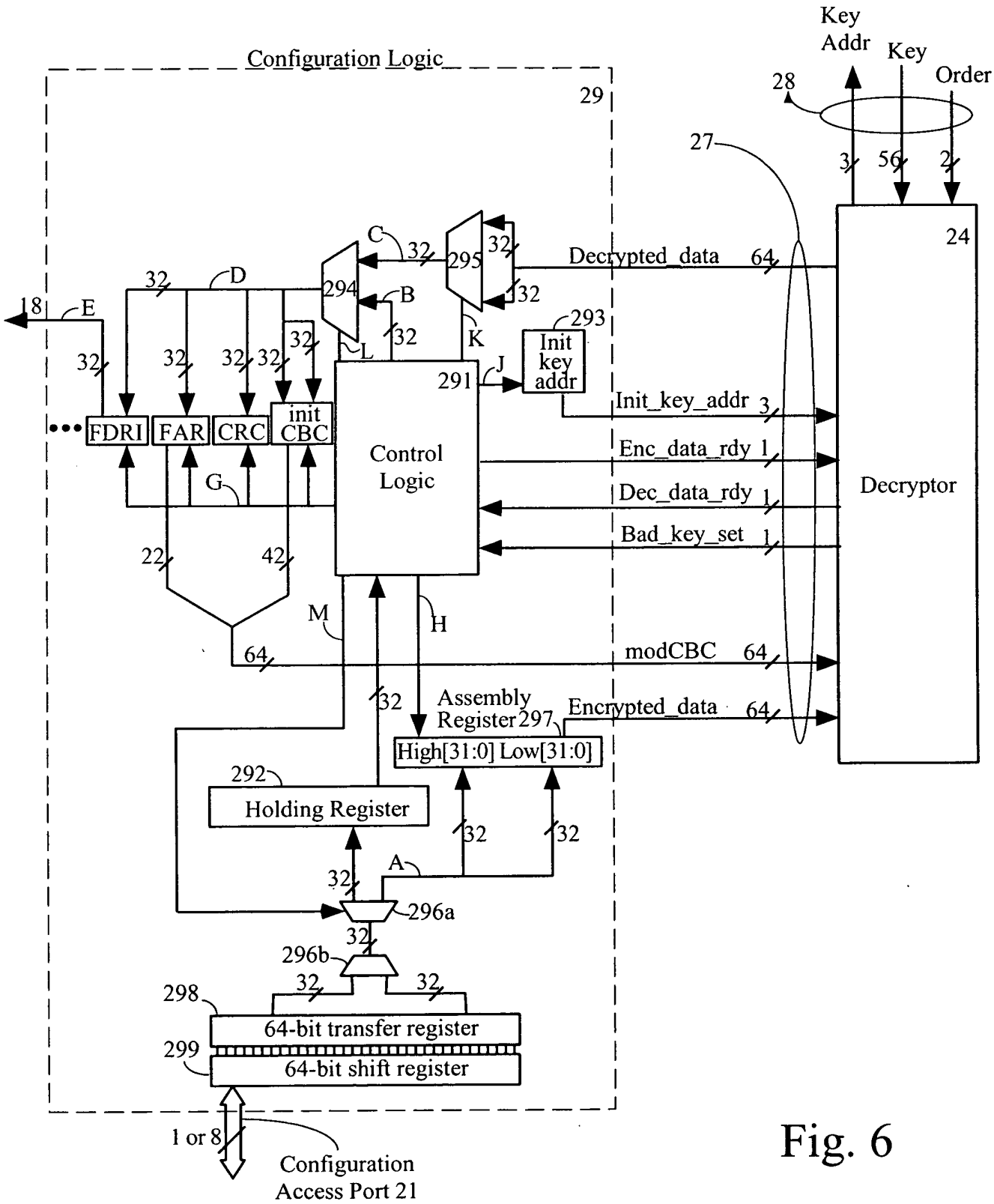

Configuration Logic
29
Key Addr
Key
Order
28
27
3
56
2
24
Decrypted_data
64
C
32
295
32
32
D
294
B
18
E
293
Init key addr
K
L
J
291
Init_key_addr
3
FDRI
FAR
CRC
init CBC
Control Logic
Enc_data_rdy
1
Dec_data_rdy
1
Bad_key_set
1
Decryptor
G
22
42
M
H
64
modCBC
64
Assembly Register
297
Encrypted_data
64
High[31:0] Low[31:0]
292
Holding Register
A
296a
296b
298
64-bit transfer register
299
64-bit shift register
1 or 8
Configuration Access Port 21

Fig. 6

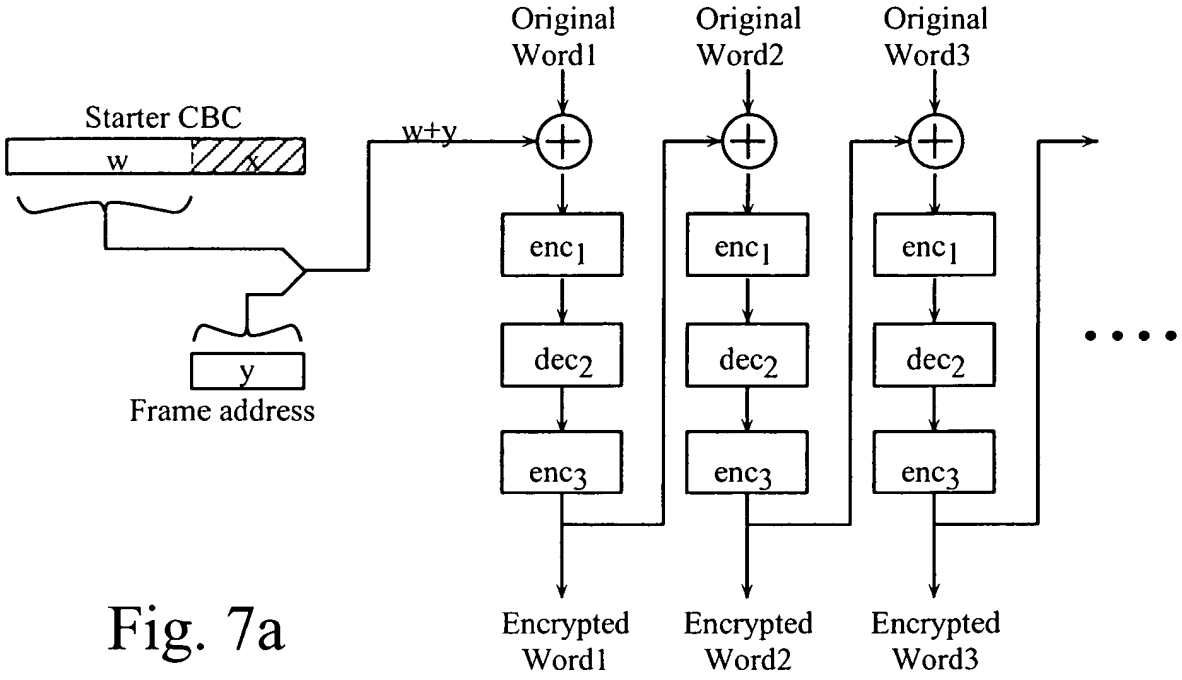

Original Word1
Original Word2
Original Word3
Starter CBC
w
x
w+y
enc1
dec2
enc3
y
Frame address
Encrypted Word1
Encrypted Word2
Encrypted Word3

Fig. 7a

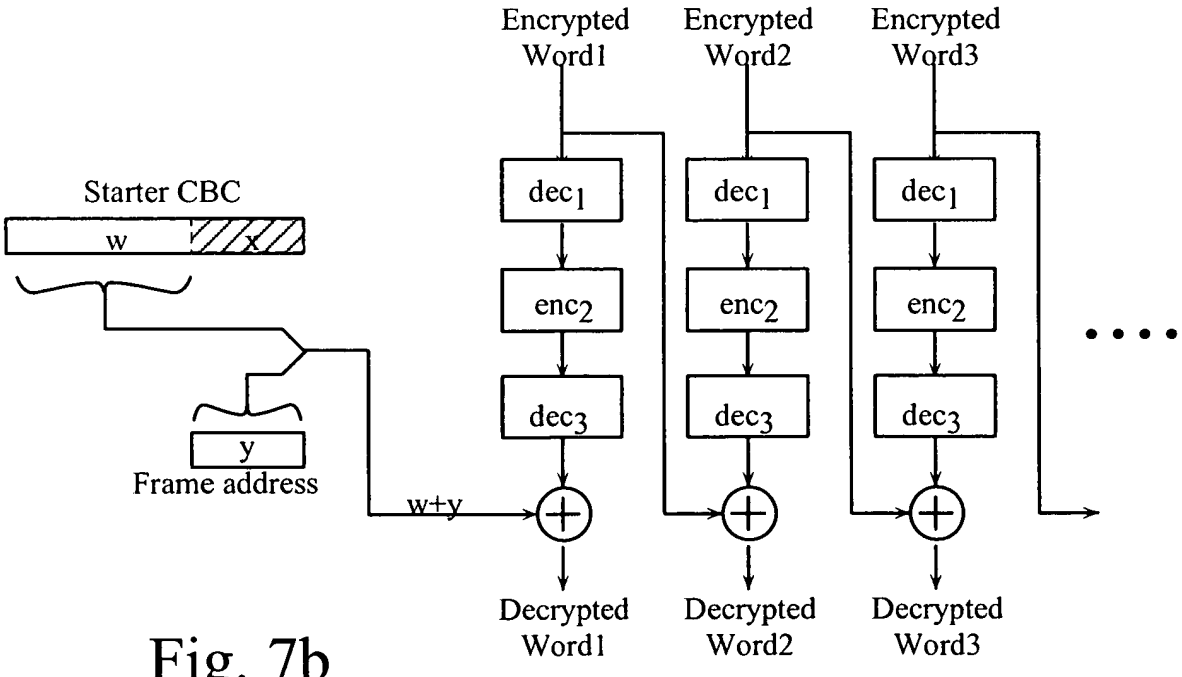

Encrypted Word1
Encrypted Word2
Encrypted Word3
Starter CBC
w
x
dec1
enc2
dec3
y
Frame address
w+y
Decrypted Word1
Decrypted Word2
Decrypted Word3

Fig. 7b

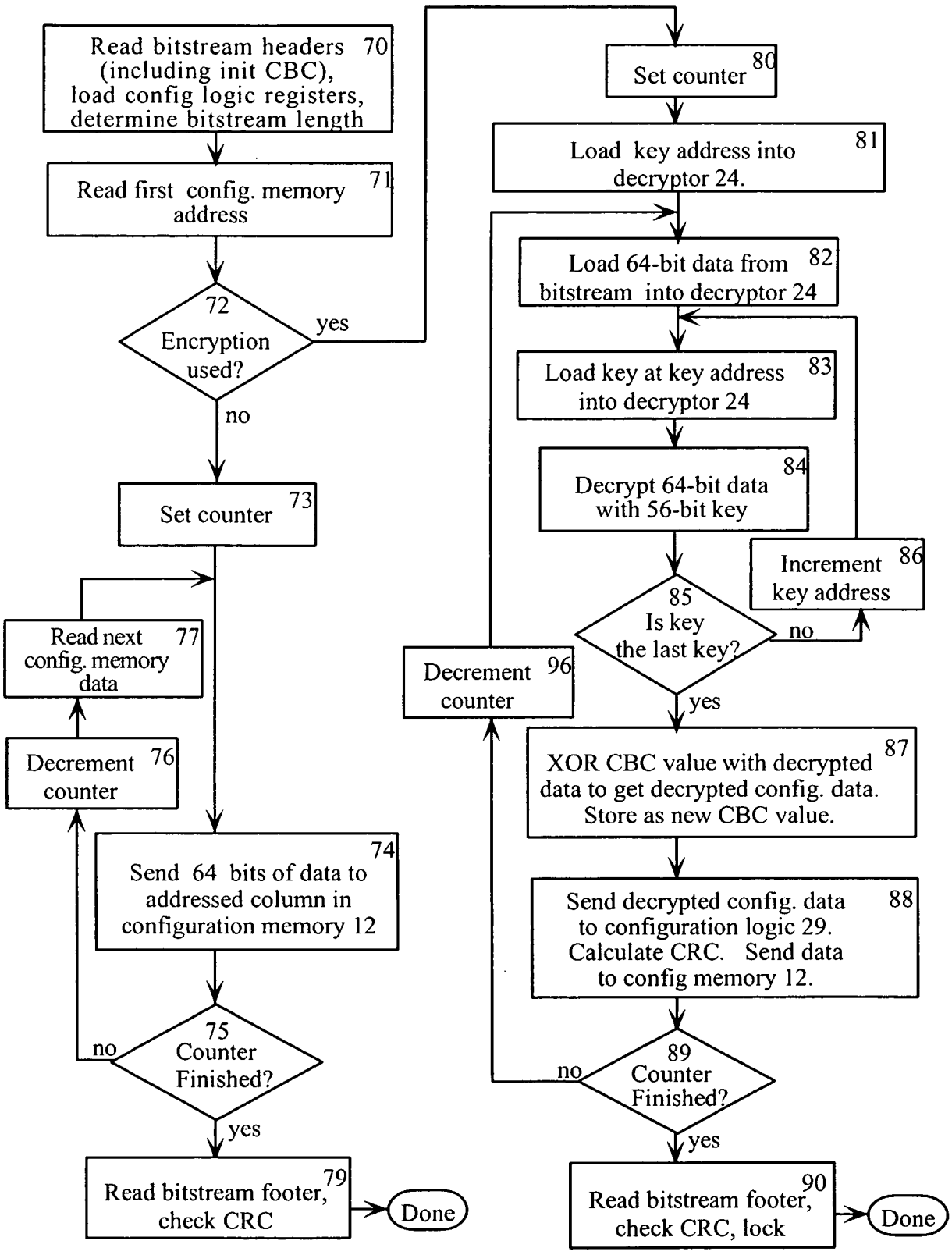

Read bitstream headers (including init CBC), load config logic registers, determine bitstream length 70
Read first config. memory address 71
72 Encryption used?
yes
no
Set counter 73
Read next config. memory data 77
Decrement counter 76
Send 64 bits of data to addressed column in configuration memory 12 74
75 Counter Finished?
no
yes
Read bitstream footer, check CRC 79
Done
Set counter 80
Load key address into decryptor 24. 81
Load 64-bit data from bitstream into decryptor 24 82
Load key at key address into decryptor 24 83
Decrypt 64-bit data with 56-bit key 84
85 Is key the last key?
no
Increment key address 86
yes
XOR CBC value with decrypted data to get decrypted config. data. Store as new CBC value. 87
Send decrypted config. data to configuration logic 29. Calculate CRC. Send data to config memory 12. 88
89 Counter Finished?
no
Decrement counter 96
yes
Read bitstream footer, check CRC, lock 90
Done

Fig. 8

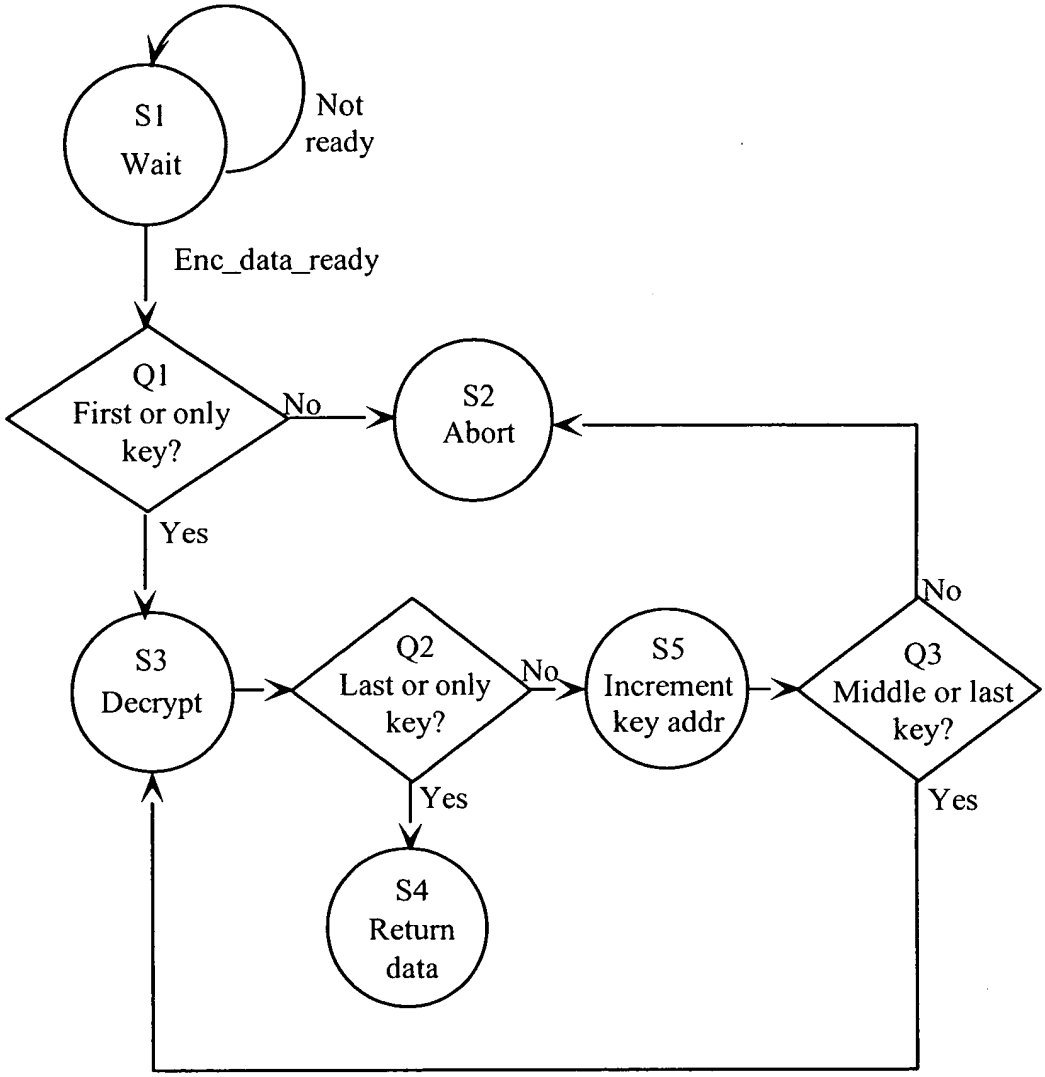

S1
Wait
Not
ready
Enc_data_ready
Q1
First or only
key?
No
S2
Abort
Yes
S3
Decrypt
Q2
Last or only
key?
No
S5
Increment
key addr
Q3
Middle or last
key?
No
Yes
Yes
S4
Return
data

Fig. 9

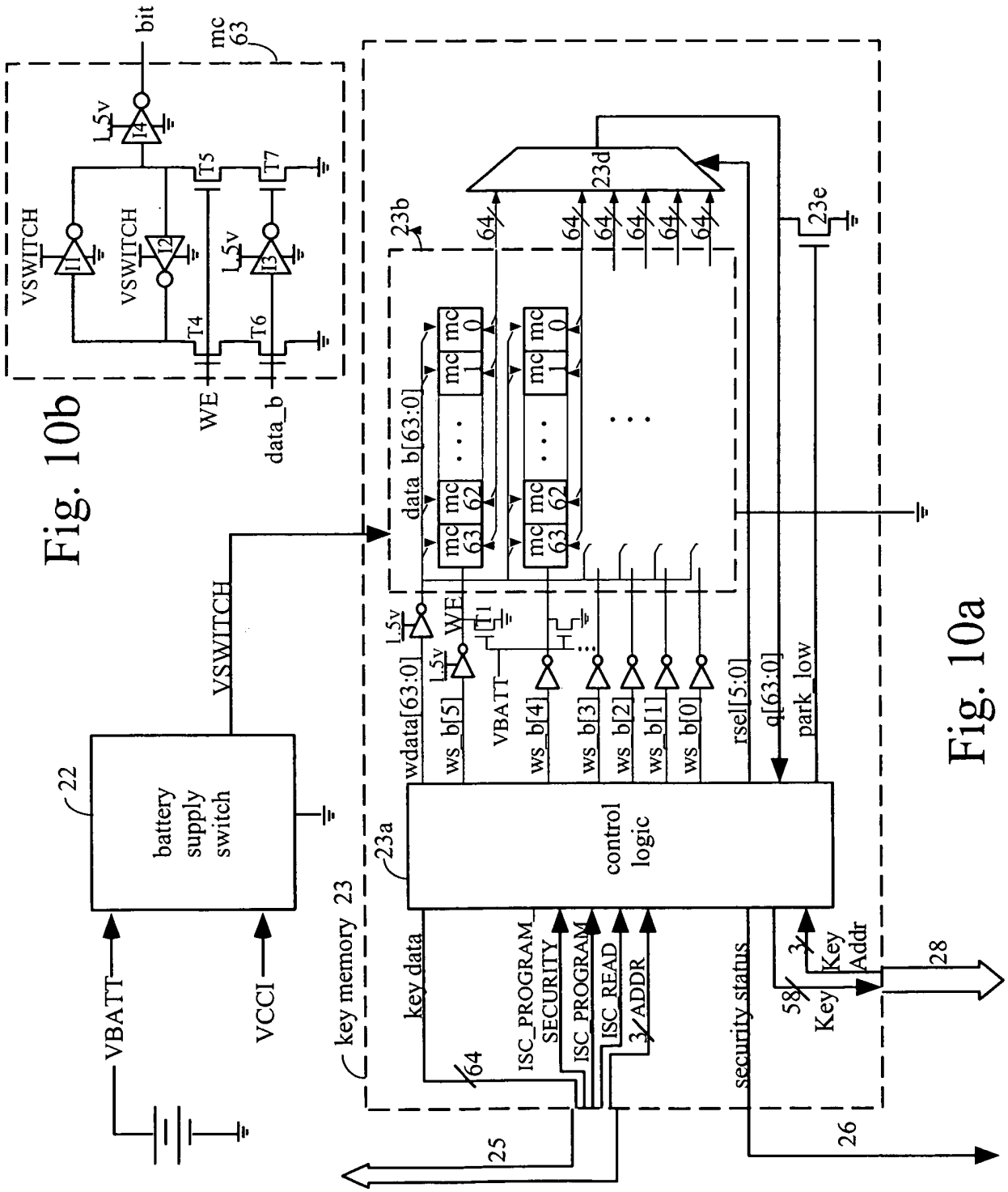


Fig. 10b

Fig. 10a

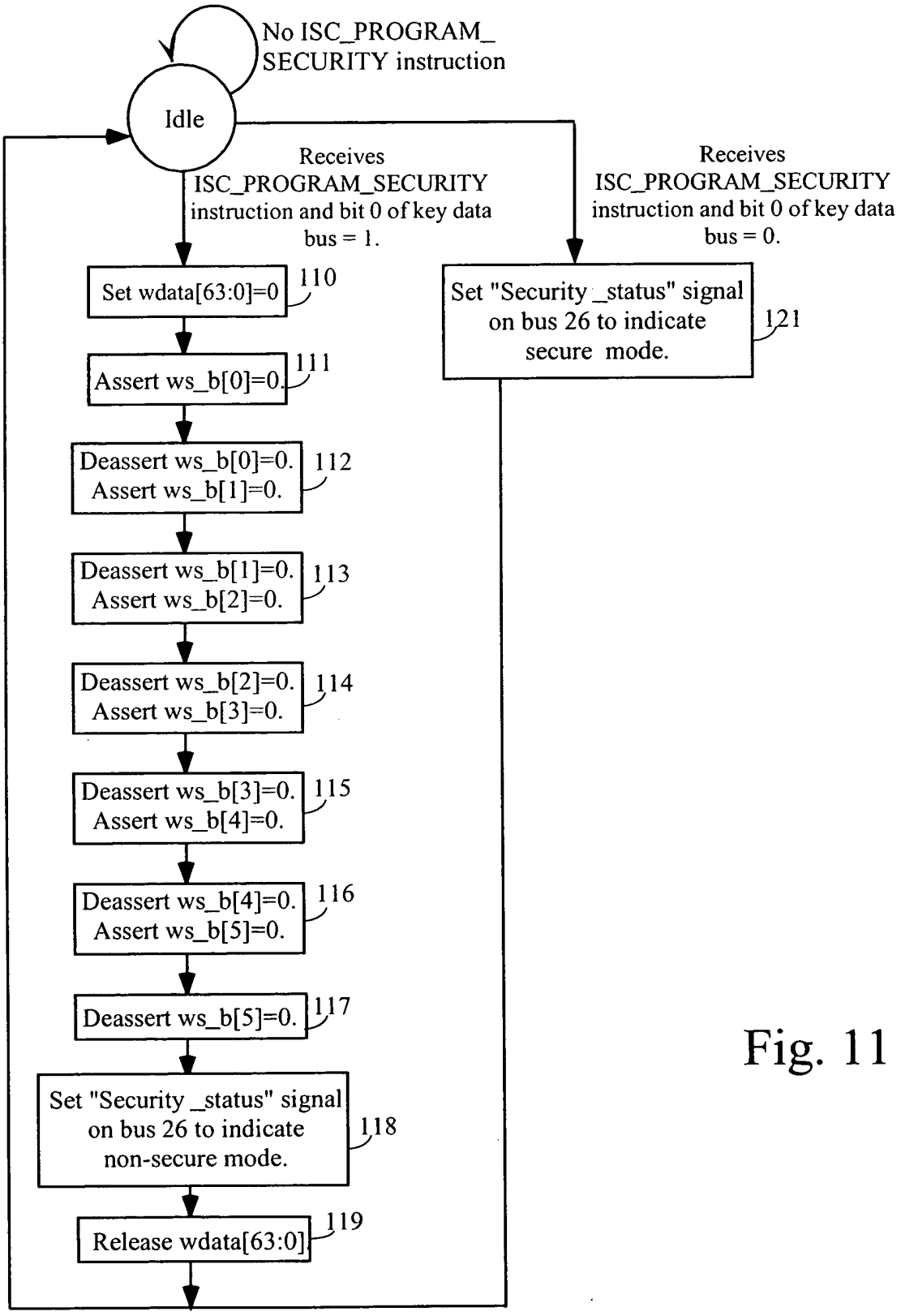

No ISC_PROGRAM_ SECURITY instruction
Idle
Receives ISC_PROGRAM_SECURITY instruction and bit 0 of key data bus = 1.
Receives ISC_PROGRAM_SECURITY instruction and bit 0 of key data bus = 0.
Set wdata[63:0]=0
110
Assert ws_b[0]=0.
111
Deassert ws_b[0]=0. Assert ws_b[1]=0.
112
Deassert ws_b[1]=0. Assert ws_b[2]=0.
113
Deassert ws_b[2]=0. Assert ws_b[3]=0.
114
Deassert ws_b[3]=0. Assert ws_b[4]=0.
115
Deassert ws_b[4]=0. Assert ws_b[5]=0.
116
Deassert ws_b[5]=0.
117
Set "Security _status" signal on bus 26 to indicate non-secure mode.
118
Release wdata[63:0]
119
Set "Security _status" signal on bus 26 to indicate secure mode.
121

Fig. 11

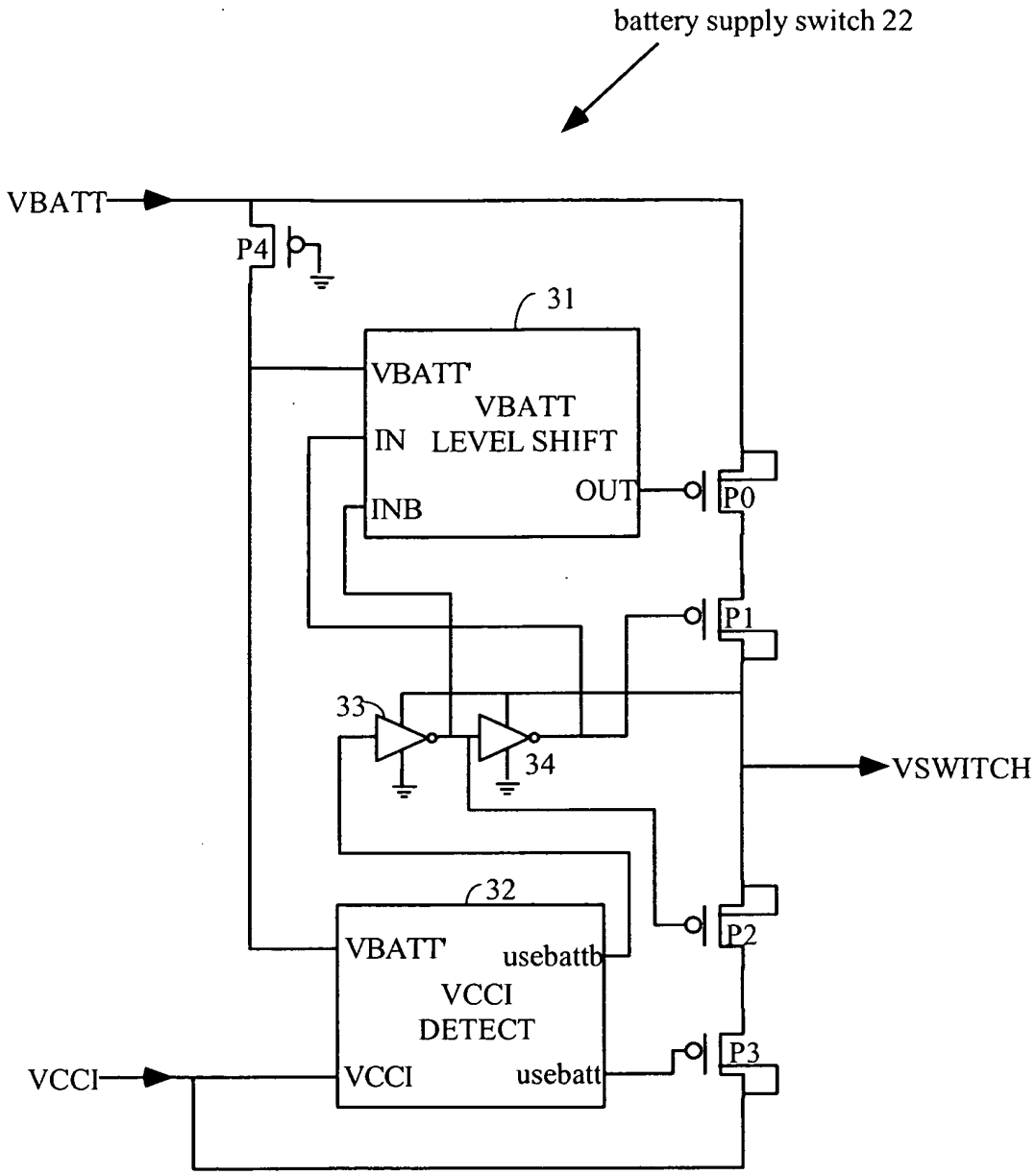

battery supply switch 22
VBATT
P4
31
VBATT
VBATT
IN
LEVEL SHIFT
OUT
INB
P0
P1
33
34
VSWITCH
32
VBATT
usebattb
VCCI
DETECT
P2
P3
VCCI
VCCI
usebatt

Fig. 12

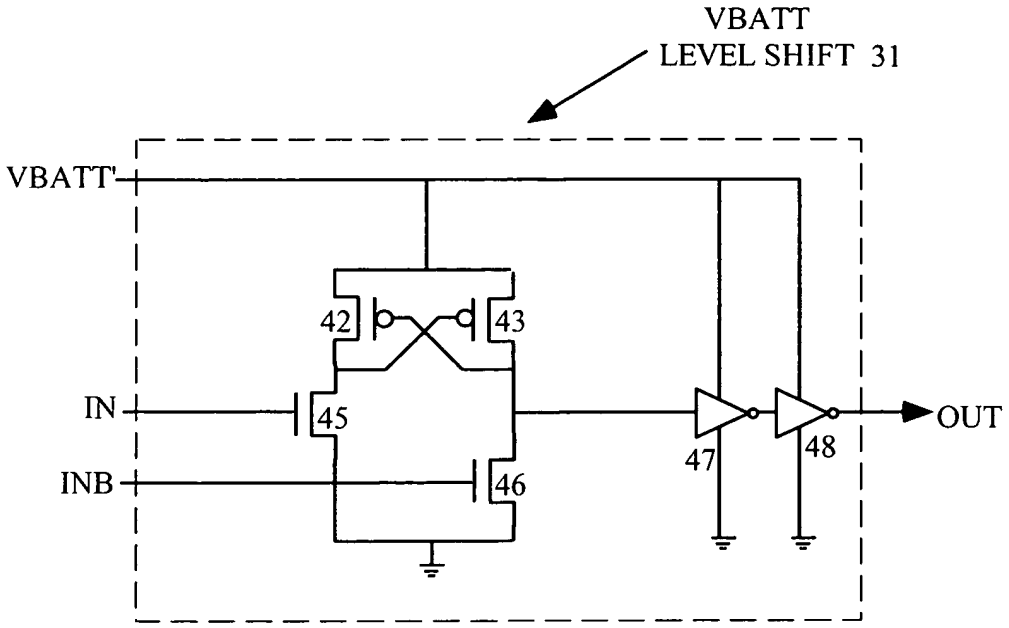

VBATT
LEVEL SHIFT 31
VBATT'
42
43
IN
45
INB
46
47
48
OUT

Fig. 13

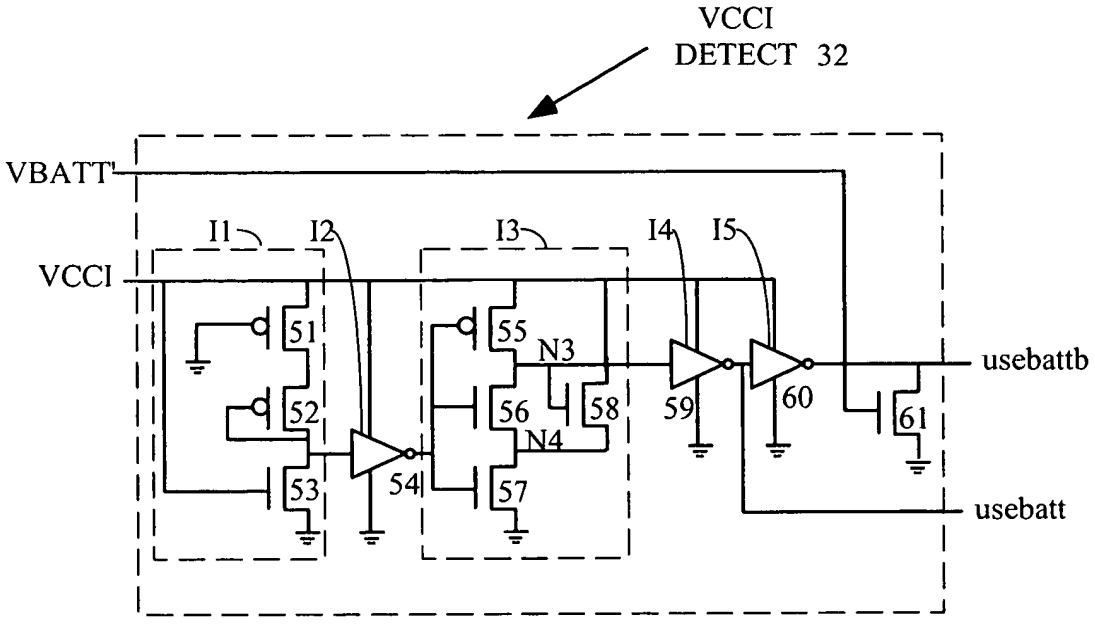

VCCI
DETECT 32
VBATT'
I1
I2
I3
I4
I5
VCCI
51
52
53
54
55
N3
56
N4
57
58
59
60
61
usebattb
usebatt

Fig. 14

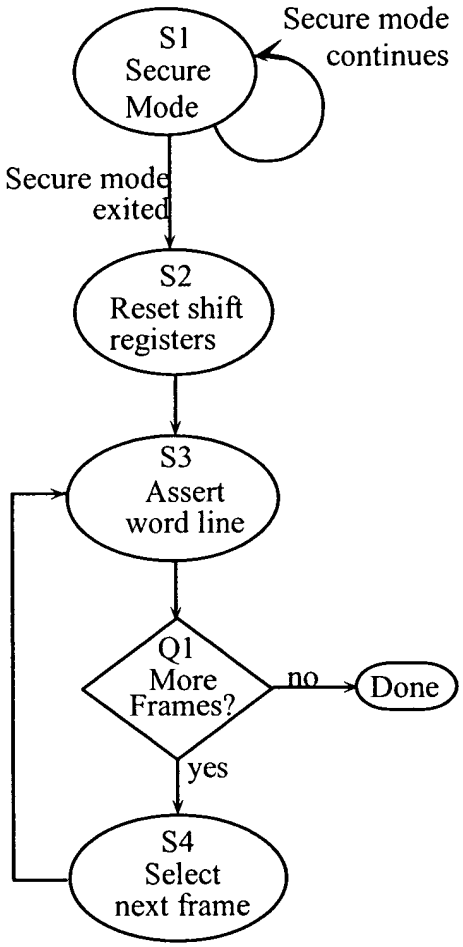

S1
Secure
Mode
Secure mode
continues
Secure mode
exited
S2
Reset shift
registers
S3
Assert
word line
Q1
More
Frames?
no
Done
yes
S4
Select
next frame

Fig. 15

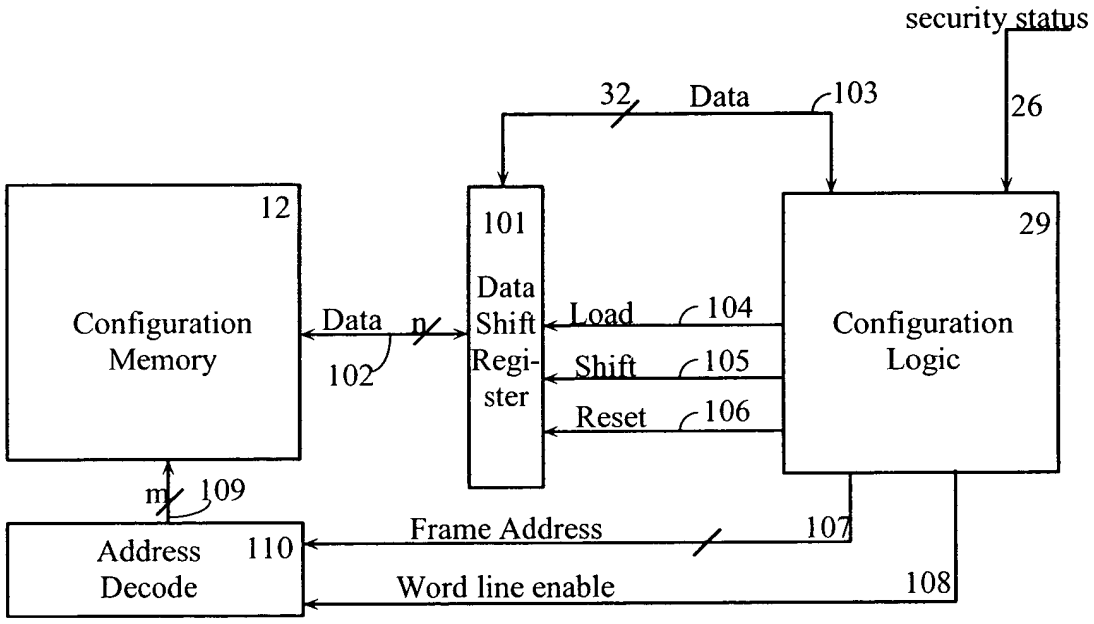

security status
26
32
Data
103
12
Configuration Memory
Data
n
102
101
Data Shift Regi-ster
Load
104
Shift
105
Reset
106
29
Configuration Logic
m
109
Address Decode
110
Frame Address
107
Word line enable
108

Fig. 16